REMARKS

Reconsideration of the Application is requested.

Claim Rejections - 35 USC § 102

"Claims 1-22 are rejected under 35 USC 102(b) as being anticipated by Want et al. (US 5,564,070)."

"Claim 1 is also rejected under 35 USC 102(e) as being anticipated by Diamant et al. (US 6,202,153)."

Applicant's Response

Applicant has cancelled claims 2, 3, 12, 19 and 20.

Applicant has amended claims 1, 18 21 and 22 for clarification.

Applicant has added claims 22 and 23.

The aim of the present invention is to protect access to personal computer applications of a computer station connected to an inter-computer communication network, for example a personalized e-mail, a financial account or other personalized applications. Normally access to personal applications is automatic when a personal portable object is near to a read unit connected to the station. This object can be preferably a wristwatch, a bracelet, a necklace, a ring, a card or a badge. In the method of claim 1, the identification code specific to the portable object, i.e. the readable word of a memory of the electronic circuit of the object, has to be searched after transmission to a determined server in a checking file. This server is, for example, the server of the watch manufacturer, which is in a particular distance from the computer station with the read unit connected to said computer station. If the readable word

has been found in the checking file, a password is sent from the checking file to the storage means in which access words are kept secret by a read and/or write barrier in order to allow opening the read barrier. If no password is transmitted, access words are kept secret, thereby guaranteeing the security of personal information stored in the portable object.

There are two checking operations to allow opening the read and/or write barrier of the storage means. First, the readable verification word of the portable object is checked in a file of the server before sending a password. Second, the password is checked to the storage means in order to open the read and/or write barrier of storage means. This method makes said object inactive, in the event of loss or theft of the portable object, by ending its validity via any communication means related to the determined server. Therefore, personal computer applications can not be opened by the loss or theft object in inactive state.

US 5,564,070 describes a method and system for maintaining processing continuity to mobile computers in a wireless network. For that, a personalised portable tab (PDA) includes a signal transmission and a reception means in order to communicate wireless with read units (IR transceivers) connected to computer stations in different rooms. This system is a ubiquitous computing environment. The personal tab includes a display in order to indicate the location of said tab in the environment, and it can communicate addresses of applications with an identification number in order to allow an agent of a computer station to recognize said personal tab. The agent is able to control the authorisation of any application to request communication with the specific mobile unit which is the personal tab. If some applications are personalised for a specific tab, the agent manages this communication between the tab and the computer application, which method is entirely different from the present invention.

Column 21, lines 1-49 specifies that the transmission from the tab of an application address packet to the computer station, and a request to introduce or modify a password of the user. A tab with a storage means that includes a read and/or write barrier to prevent access to specific applications of the computer without authorisation is not described, although such is present in the present invention. This barrier can be opened only if a verification word in a readable part of the storage means has been checked in a checking file located in a server not directly connected to the computer station, but connected by Internet for example to the computer station. This procedure for sending the verification word is automatic since the tab or portable object is located near the read unit. Once the verification word has been found in the checking file of the server, a password from the server is transmitted to the electronic circuit of the portable object in order to open the read and/or write barrier of the storage means. After that, application addresses can be transmitted from the storage means of the portable object to the computer station to open said personalised applications.

The Office Action notes that the tab displays "you are here" show the location of the user, which is different from steps A or C of Claim 1 of the present invention, in which an automatic connection to the server is established for checking the readable word in a list of authorised words. Further, US 5,564,070, column 7, lines 6-9 does not mentioned step B of Claim 1 of the present invention and it is not obvious for one of ordinary skill in the art to deduce this step B in light of the teaching.

Again, the present invention has two password checking operations in order to authorize the opening of personal applications. First, the readable word is checked in the checking file of the server, and second the password is checked in the storage means to open the read and/or write barrier.

We cannot compare the agent of the computer that is described in US 5,564,070 with the barrier of the storage means of the portable object of the present invention, because this agent does not transmit a password to the tab in order to eventually open a barrier to the storage means. Furthermore, this reference does not describe a check of the verification word of the portable object in a checking file of a specific server that is not an agent of the computer. This check will make the portable object inactive, by ending its validity via any communication means related to the determined server in the event of loss or theft. Thereafter, personal computer applications could not be opened by the lost or stolen object while in an inactive state.

Additionally, US 5,564,070 does not describe a read unit integrated into a case, a computer keyboard, or a mouse pad as specified in amended Claim 18. Furthermore, the portable object specified as a wristwatch according to amended Claim 21 it is not described. Therefore, Claims 1, 18, 21 and 23 are novel and based on an inventive step.

US 6,202,153 describes a security switching device. The device includes a computer system, a storage unit connected to the computer system, and a portable unit in order to communicate wireless with the computer system (column 16). An authorised user can have access to secured areas of the storage unit when the personal portable unit is close to the device (column 16, lines 49-52). It is mentioned also that a bi-directional communication can be established between the device and the portable unit to exchange decoded signals, which is different from a transmission of passwords. This reference fails to mention the readable word that is checked in a checking file of a dedicated server, and that a password is transmitted from the server to the storage means of the electronic circuit in order to open a read and/or write barrier of the storage means so that computer applications are opened. Therefore, Claims 1, 18, 21 and 23 are novel and based on an inventive step.

Conclusion

For the foregoing reasons, it is submitted that the claims are in condition for allowance, and such is respectfully solicited.

Respectfully submitted,

Date: January 19, 2005

Richard K. Robinson (PTO Reg. No. 28,109)
Harry C. Post, III (PTO Reg. No. 26,019)
Attorneys for Applicant

Robinson & Post, L.L.P.
North Dallas Bank Tower, Suite 575
12900 Preston Road, LB-41
Dallas, Texas 75230
Tel: 972-866-7786
Fax: 972-866-7787